Journal of Algebra **227,** 532–548 (2000)
doi:10.1006/jabr.1999.8168, available online at http://www.idealibrary.com on IDEAL®

Pencils of Quadratic Forms and Hyperelliptic Function Fields

David B. Leep

and

Laura Mann Schueller

Department of Mathematics, Whitman College, Walla Walla, Washington 99362

Communicated by Walter Feit

Received July 11, 1999

Let $P(k)$ denote the set of equivalence classes of nonsingular pencils of quadratic forms of even order defined over a field k, char $k \neq 2$. Let $F(k)$ denote the set of k-isomorphism classes of hyperelliptic function fields defined over k. We define a map Φ: $P(k) \to F(k)$ and determine precisely when Φ is surjective and when Φ is injective. This extends a method used by A. Weil to study pairs of quadratic forms over finite fields. © 2000 Academic Press

Key Words: hyperelliptic function field; pencil of quadratic forms; quadratic form.

1. INTRODUCTION

This paper extends a method used by Weil in [10] to study the zeta function of a pair of nonsingular quadratic forms defined over a finite field having odd characteristic. To a nonsingular pair of quadratic forms $\{F, G\}$ in an even number of variables, Weil associates the hyperelliptic function field $k(u, y)$ given by $y^2 = \det(uF + G)$. Weil closely relates the zeta function of the pair of quadratic forms to the zeta function of the hyperelliptic curve.

Let $P(k)$ denote the set of equivalence classes of nonsingular pencils of quadratic forms of even order defined over a field k, char $k \neq 2$. Let $F(k)$ denote the set of k-isomorphism classes of hyperelliptic function fields defined over k.

0021-8693/00 $35.00

The main results of this paper are to define a map Φ: $P(k) \to F(k)$ and to determine precisely when Φ is surjective and when Φ is injective. See Theorems 3.1, 4.11, and 5.6. These results lead to the paper's main theorem, Theorem 5.7.

As Weil, in [10], we deal only with pencils of quadratic forms having even order since the map Φ is not well defined when the order is odd.

2. SOME PRELIMINARIES

In this paper, we assume that k is a field with $\operatorname{char} k \neq 2$. We let $k^\times$ denote the nonzero elements of k, $(k^\times)^2$ the nonzero squares in k, and k^{alg} the algebraic closure of k.

A quadratic form F in n variables defined over k is a homogeneous polynomial of degree two in the polynomial ring $k[x_1, \ldots, x_n]$. Two quadratic forms, F, F', are equivalent over k if there exists an invertible $n \times n$ matrix $E = (e_{ij})_{n\times n}$ with entries in k such that

$$F'(x_1, \ldots, x_n) = F(y_1, \ldots, y_n), \qquad \text{for } y_i = \sum_{j=1}^{n} e_{ij}x_j, \quad 1 \leq i \leq n.$$

The order of F is the minimum m such that F is k-equivalent to a quadratic form $F' = \sum_{1 \leq i \leq j \leq m} a'_{ij}x_ix_j$. If $m < n$, then F is degenerate, and if $m = n$, then F is nondegenerate.

Let $[F]$ denote the symmetric $n \times n$ matrix $(\alpha_{ij})_{n\times n}$ where

$$\alpha_{ij} = \begin{cases} a_{ij} & i < j \\ a_{ji} & j < i \\ 2a_{ii} & i = j \end{cases}.$$

Thus,

$$[F] = \begin{pmatrix} 2a_{11} & a_{12} & \cdots & a_{1n} \\ a_{12} & & & \\ \vdots & & & \\ a_{1n} & a_{2n} & \cdots & 2a_{nn} \end{pmatrix}.$$

Let $\det(F) = \det([F])$. If F and F' are equivalent over k, then $\det(F) = c^2 \det(F')$ for $c \in k^\times$.

Let $\{F, G\}$ and $\{F', G'\}$ be two pairs of quadratic forms defined over k. The pairs are equivalent over k if both F is equivalent to F' and G is equivalent to G' by the same invertible matrix E. The order of the pair

$\{F, G\}$ is the minimum m such that there exists a pair of quadratic forms

$$\left\{F' = \sum_{1 \le i \le j \le m} a'_{ij} x_i x_j, G' = \sum_{1 \le i \le j \le m} b'_{ij} x_i x_j\right\}$$

equivalent to $\{F, G\}$. If $m < n$, then the pair $\{F, G\}$ is degenerate, and if $m = n$, then the pair $\{F, G\}$ is nondegenerate.

A pair of quadratic forms $\{F, G\}$ defined over k is nonsingular if there exists no singular zero of the pair over k^{alg}.

If a nonsingular pair $\{F, G\}$ has order n and u is an indeterminate over k, then $\det(uF + G)$ splits into either $n - 1$ or n distinct linear factors over k^{alg} depending on whether F is degenerate or not.

The pencil of $\{F, G\}$, denoted $P(F, G)$, is the set of all nonzero k-linear combinations of F and G.

Let $\{F, G\}$ and $\{F', G'\}$ be two pairs of quadratic forms. The two pencils $P(F, G)$ and $P(F', G')$ are k-equivalent if there exist $a, b, c, d \in k$ with $ad - bc \neq 0$ such that the pair $\{F, G\}$ is equivalent to the pair $\{aF' + bG', cF' + dG'\}$. This is an equivalence relation on the set of pencils of forms defined over a given field k.

We say that a pencil $P(F, G)$ is nonsingular if the pair $\{F, G\}$ is nonsingular. Further, we say that the order of the pencil is equal to the order of the pair $\{F, G\}$. Both of these notions are well defined on the pencil.

We define F to be a hyperelliptic function field over k if

1. $F = k(u, y)$,
2. u is transcendental over k,
3. $[k(u, y) : k(u)] = 2$, and
4. the constant field of F is k (k is algebraically closed in F).

When the genus of F is at least two, this definition is equivalent to the one given by Stichtenoth in [8, p. 193]. For convenience of terminology, we include function fields of genus zero or one in our definition of hyperelliptic function fields. When the genus is at least two, our definition is not the same as the definition given by Chevalley in [1, p. 74].

LEMMA 2.1. *Suppose that $k(u, y)$ and $k(u', y')$ are k-isomorphic hyperelliptic function fields and assume one of the following*:

1. $y^2 = f(u) \in k[u]$, $(y')^2 = g(u') \in k[u']$, *and* $\deg f = \deg g = 3$, *or*
2. *the genus of $k(u, y)$ is zero and k is quadratically closed.*

Then, there exists a k-isomorphism θ: $k(u, y) \to k(u', y')$ such that $\theta(k(u)) = k(u')$.

Proof. Since $k(u, y)$ is k-isomorphic to $k(u', y')$, there is a k-isomorphism $\tau\colon k(u, y) \to k(u', y')$. Thus, it is sufficient to show that there exists a k-automorphism, $\sigma\colon k(u', y') \to k(u', y')$ such that $\sigma(\tau(k(u))) = k(u')$. Letting $\theta = \sigma \circ \tau$, we would have the desired isomorphism.

In the first case, the result follows from Lemma 4.4 in [2, p. 318].

In the second case, $k(u', y') = k(x)$ for some $x \in k(u', y')$. It is sufficient to show that if $E_1, E_2 \subseteq k(x)$ with $[k(x)\colon E_1] = [k(x)\colon E_2] = 2$, then there exists a k-automorphism $\sigma\colon k(x) \to k(x)$ such that $\sigma(E_1) = E_2$.

For $i = 1, 2$, let $\mathrm{Gal}(k(x)/E_i) = \{1, \lambda_i\}$. It is sufficient to find $\sigma \in \mathrm{Gal}(k(x)/k)$ such that $\sigma\lambda_1\sigma^{-1} = \lambda_2$.

Recall that $\mathrm{Gal}(k(x)/k)$ is k-isomorphic to $PGL_2(k)$ by the isomorphism that takes σ to $A_\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where $\sigma(x) = \frac{ax + b}{cx + d}$. Since λ_1 and λ_2 each have order 2, one can show that A_{λ_1} and A_{λ_2} each have trace zero. Since $k^\times = (k^\times)^2$ and A_{λ_2} is determined only up to multiplication by a constant multiple of the identity matrix, we may assume $\det(A_{\lambda_1}) = \det(A_{\lambda_2})$. Since A_{λ_1} and A_{λ_2} have the same characteristic polynomial and the characteristic polynomial has distinct roots, it follows that λ_1 and λ_2 are conjugate over k. ∎

PROPOSITION 2.2. *Let $k(u, y)$ be the hyperelliptic function field given by $(y^2 = f(u) \in k[u]$, and let $k(u', y')$ be the hyperelliptic function field given by $(y')^2 = g(u') \in k[u']$.*

1. *If $g(u') = f((au' + c)/(bu' + d))h(u')^2$ for some $h(u') \in k(u')^\times$ and some $a, b, c, d \in k$ with $ad - bc \neq 0$, then $k(u, y)$ and $k(u', y')$ are k-isomorphic.*

2. *If $k(u, y)$ and $k(u', y')$ are k-isomorphic and either*

   (a) *the genus of $k(u, y)$ is at least two,*

   (b) *the genus of $k(u, y)$ is zero and k is quadratically closed, or*

   (c) *$f(u)$ and $g(u')$ have degree 3,*

then $g(u') = f((au' + c)/(bu' + d))h(u')^2$ for some $h(u') \in k(u')^\times$ and $a, b, c, d \in k$ with $ad - bc \neq 0$.

Proof. (1) If $g(u') = f((au' + c)/(bu' + d))h(u')^2$ for some nonzero $h(u') \in k(u')$ and some $a, b, c, d \in k$ with $ad - bc \neq 0$, then we can define a k-isomorphism

$$\theta\colon k(u, y) \to k(u', y')$$

by $\theta(u) = (au' + c)/(bu' + d)$ and $\theta(y) = y'/h(u')$.

(2) Assume that $k(u, y)$ and $k(u', y')$ are k-isomorphic. By Proposition VI.2.4 in [8], if $g \geq 2$ or by Lemma 2.1 otherwise, there exists a k-isomorphism

$$\theta\colon k(u, y) \to k(u', y')$$

such that $\theta(k(u)) = k(u')$.

Given such a θ, $\theta(u) = (au' + c)/(bu' + d)$ for some $a, b, c, d \in k$ with $ad - bc \neq 0$. In general, $\theta(y) = h_1(u')y' + h_2(u')$, with $h_1, h_2 \in k(u')$. Since $y \notin k(u)$, we have $\theta(y) \notin k(u')$ and it follows that $h_1(u') \neq 0$. Further, since

$$\theta(y^2) = h_1(u')^2(y')^2 + 2h_1(u')h_2(u')y' + h_2(u')^2 \in k(u')$$

and $(y')^2 \in k(u')$, it follows that $h_2(u') = 0$. Let $h(u') = 1/h_1(u')$. Since,

$$\theta(y^2) = (y')^2/(h(u'))^2 = g(u')/(h(u'))^2$$

and

$$\theta(y^2) = \theta(f(u)) = f(\theta(u)) = f\left(\frac{au' + c}{bu' + d}\right),$$

it follows that $g(u') = f((au' + c)/(bu' + d))(h(u'))^2$. ∎

3. THE MAP

Define $F(k)$ to be the set of hyperelliptic function fields over the field k up to k-isomorphism and let $P(k)$ be the set of equivalence classes of even order, nonsingular pencils of quadratic forms defined over k.

Let $P(F, G)$ represent an element in $P(k)$. Then, $\det(uF + G)$ is a square free polynomial in $k[u]$, and $k(u, y)$ given by $y^2 = \det(uF + G)$ is a hyperelliptic function field.

THEOREM 3.1. *The map*

$$\Phi\colon P(k) \to F(k)$$

defined by $\Phi(P(F, G)) = k(u, y)$, *where* $y^2 = \det(uF + G)$, *is well defined.*

Proof. Let $P(F, G)$ and $P(F', G')$ be equivalent, nonsingular pencils of order n defined over k, where n is even. Then, there exist $a, b, c, d \in k$ with $ad - bc \neq 0$ and an invertible $n \times n$ matrix E with entries in k such that

$$[F'] = E[aF + bG]E^t \qquad \text{and} \qquad [G'] = E[cF + dG]E^t.$$

Then, $\det(u'F' + G') = \det(E)^2(u'b + d)^n \det(((u'a + c)/(u'b + d))F + G)$. By Proposition 2.2(1), we have $\Phi(P(F, G)) = \Phi(P(F', G'))$, and the map is well defined. ∎

4. SURJECTIVITY

Let $p(x)$ be an irreducible monic polynomial over k, $L = k[x]/p(x)$, and let $s: L \to k$ be any nonzero k-linear map. For any basis $\{v_1, \ldots, v_n\}$ of L over k and any $\alpha \in L^\times$, we can define the quadratic form, $s_*(\langle \alpha \rangle)$, over k by

$$s_*(\langle \alpha \rangle) = \sum_{1 \le i < j \le n} 2s(\alpha v_i v_j) x_i x_j + \sum_{1 \le i \le n} s(\alpha v_i^2) x_i^2.$$

Let $L^* = \mathrm{Hom}_k(L, k)$. For any $\alpha \in L^\times$, define $\rho_\alpha: L \to L^*$ to be the k-vector space isomorphism given by $\rho_\alpha(v)(w) = s(\alpha vw)$ for all $v, w \in L$.

LEMMA 4.1. *Let $\theta = x + (p(x)) \in L$ be a root of $p(x)$. Let $F = s_*(\langle \alpha \rangle)$ and $G = s_*(\langle -\theta\alpha \rangle)$. Then*

$$\det(uF + G) = (\det F)p(u).$$

Proof. Let T be the k-linear transformation of L that represents multiplication by θ. For any $v, w \in L$,

$$\begin{aligned} \rho_{-\theta\alpha}(v)(w) &= s(-\theta\alpha vw) = -s(\alpha\theta vw) \\ &= -s(\alpha(Tv)w) = -\rho_\alpha(Tv)(w). \end{aligned}$$

Therefore $\rho_\alpha^{-1}\rho_{-\theta\alpha} = -T$ and as matrices $F^{-1}G = -T$.

Let $g(u) = \det(uI - T)$. Then

$$\begin{aligned} \det(uF + G) &= (\det F)\det(uI + F^{-1}G) \\ &= (\det F)\det(uI - T) = (\det F)g(u). \end{aligned}$$

The Cayley–Hamilton theorem implies that $g(T) = 0$. Since for every $v \in L$, $0 = g(T)v = g(\theta)v$, we have $g(\theta) = 0$. Since $p(u)$ is the minimal polynomial for θ, $p(u)$ divides $g(u)$. Further, since $p(u)$ and $g(u)$ are monic and have degree equal to $[L : k]$, we have $g(u) = p(u)$. Therefore, $\det(uF + G) = (\det F)g(u) = (\det F)p(u)$. ∎

LEMMA 4.2.

$$\det(s_*(\langle \alpha \rangle)) = N_{L/k}(\alpha)\det(s_*(\langle 1 \rangle)).$$

Proof. This result is given in [6, p. 51]. ∎

LEMMA 4.3. *Let $\{F, G\}$ be a nonsingular pair of forms with* $\det(uF + G) = cp(u)$ *for $c \in k^\times$. There exist $\alpha \in L^\times$ and $\theta \in L^\times$, a root of $p(u)$, such that $F = s_*(\langle \alpha \rangle)$ and $G = s_*(\langle -\theta\alpha \rangle)$.*

Proof. Variations of this result are given in [3, 5, 7, 9]. ∎

LEMMA 4.4. *Let $\alpha, \beta \in L^\times$. Let $\theta \in L^\times$ be a root of $p(x)$. The following are equivalent.*

1. *The pair $\{s_*(\langle \alpha \rangle), s_*(\langle -\theta\alpha \rangle)\}$ is equivalent to the pair*

$$\{s_*(\langle \beta \rangle), s_*(\langle -\theta\beta \rangle)\}.$$

2. *There exists $\gamma \in L^\times$ such that $\alpha = \gamma^2\beta$.*

3. *There exists a k-linear transformation $\tau\colon L \to L$ such that for all $v, w \in L$, $s(\alpha vw) = s(\beta\tau(v)\tau(w))$ and $s(-\theta\alpha vw) = s(-\theta\beta\tau(v)\tau(w))$.*

Proof. This result is given in [7]. For (3) implies (2), one observes that a k-linear transformation, as in (3), is multiplication by some $\gamma \in L^\times$. ∎

For an arbitrary finite extension L/k, let $N_{L/k}\colon L^\times \to k^\times$ be the norm map and let $\overline{N}_{L/k}\colon L^\times/(L^\times)^2 \to k^\times/(k^\times)^2$ be the induced map. If $[L : k] = n$ is odd, then $\overline{N}_{L/k}$ is surjective since for all $a \in k^\times$, we have $\overline{N}_{L/k}(a(L^\times)^2) = a^n(k^\times)^2 = a(k^\times)^2$.

PROPOSITION 4.5. *If k is perfect and $\overline{N}_{L/k}$ is surjective for every finite extension L/k, then Φ is surjective.*

Proof. Let $k(u, y) \in F(k)$ with $y^2 = c\prod_{i=1}^m p_i(u)$ where the $p_i(u)$'s are distinct monic irreducible polynomials and $c \in k^\times$.

Let $L_i = k[u]/p_i(u)$ and let $\theta_i = u + (p_i(u)) \in L_i$ be a root of $p_i(u)$. Let $s_i\colon L_i \to k$ be a nonzero k-linear map. Using the surjectivity of the maps $\overline{N}_{L_i/k}$, choose $\alpha_i \in L_i$ such that

$$\overline{N}_{L_i/k}(\alpha_i) \in \begin{cases} \left(\dfrac{c}{\det((s_i)_*(\langle 1 \rangle))}\right)(k^\times)^2 & i = 1 \\ \left(\dfrac{1}{\det((s_i)_*(\langle 1 \rangle))}\right)(k^\times)^2 & i = 2, 3, \ldots, m. \end{cases}.$$

Let $F_i = (s_i)_*(\langle \alpha_i \rangle)$ and $G_i = (s_i)_*(\langle -\theta_i\alpha_i \rangle)$, $1 \le i \le m$, and let

$$F = F_1 \oplus \cdots \oplus F_m, \qquad G = G_1 \oplus \cdots \oplus G_m.$$

Then, by Lemmas 4.1 and 4.2,

$$\det(uF + G) = \prod_{i=1}^{m} (\det F_i)\, p_i(u) = \prod_{i=1}^{m} N_{L_i/k}(\alpha_i) \det\big((s_i)_*(\langle 1\rangle)\big)\, p_i(u)$$

$$= cd^2 \prod_{i=1}^{m} p_i(u) \qquad \text{for some } d \in k^\times.$$

Let $n = \sum_{i=1}^{m} \deg(p_i)$. Then the pair $\{F, G\}$ has order n.

The pair $\{F, G\}$ is nonsingular since $\det(uF + G)$ has n distinct roots. If n is even, then $P(F, G) \in P(k)$ and $\Phi(P(F, G)) = k(u, y)$.

If n is odd, then define $F_0 = 0x^2$ and $G_0 = x^2$. Let $\overline{F} = F_0 \oplus F$ and let $\overline{G} = G_0 \oplus G$. Then, the pair $\{\overline{F}, \overline{G}\}$ has order $n + 1$ and $\det(u\overline{F} + \overline{G}) = cd^2 \prod_{i=1}^{m} p_i(u)$ has n distinct roots.

The pair $\{\overline{F}, \overline{G}\}$ is nonsingular and has even order, and $\Phi(P(\overline{F}, \overline{G})) = k(u, y)$.

Therefore, Φ is surjective. ∎

LEMMA 4.6. *Let $k(u, y)$ be the hyperelliptic function field defined by $y^2 = f(u)$ where $f(u) \in k[u]$ has distinct roots in k^{alg}. Assume either*

1. *the genus of $k(u, y)$ is at least two,*
2. *the genus of $k(u, y)$ is zero and k is quadratically closed, or*
3. $\deg(f) = 3$.

Assume $P(F, G) \in P(k)$ and $\Phi(P(F, G)) = k(u, y)$. Then, there exist $h \in k^\times$ and $F', G' \in P(F, G)$ such that

$$\det(uF' + G') = h^2 f(u).$$

Proof. By Proposition 2.2(2),

$$\det(uF + G) = f\left(\frac{au + b}{cu + d}\right) g(u)^2$$

for some $a, b, c, d \in k$ with $ad - bc \neq 0$ and some $g(u) \in k(u)^\times$. Since the order of $\{F, G\}$ is even, it follows some $F', G' \in P(F, G)$ and $h(u) \in k(u)^\times$, that $\det(uF' + G') = f(u)h(u)^2$. Since the pair $\{F', G'\}$ is nonsingular, $f(u)h(u)^2$ is a square-free polynomial in $k[u]$. Therefore $h(u) = h \in k^\times$. ∎

LEMMA 4.7. *Let $\{F, G\}$ be a nonsingular pair of quadratic forms over k and suppose $\det(uF + G) = p_1(u)p_2(u)$ where $\gcd(p_1(u), p_2(u)) = 1$. Then, $F = F_1 \oplus F_2$ and $G = G_1 \oplus G_2$ with $\det(uF_1 + G_1) = c_1 p_1(u)$ and $\det(uF_2 + G_2) = c_2 p_2(u)$ for some $c_1, c_2 \in k^\times$.*

Proof. This result is given in [5, 7, 9]. ∎

LEMMA 4.8. *If k is formally real, then Φ is not surjective.*

Proof. Suppose k is formally real. Let $k(u', y')$ be the hyperelliptic function field given by

$$(y')^2 = \big((u')^2 + 1\big)\big((u')^2 + 2\big)\big((u')^2 + 3\big).$$

Suppose $\Phi(P(F, G)) = k(u', y')$.

Since the genus of $k(u', y')$ is two, Lemma 4.6 implies there exist $h \in k^\times$ and $F', G' \in P(F, G)$ such that

$$\det(uF' + G') = h^2(u^2 + 1)(u^2 + 2)(u^2 + 3).$$

Lemma 4.7 implies that $\{F', G'\} = \{F_1 \oplus F_2 \oplus F_3, G_1 \oplus G_2 \oplus G_3\}$ with

$$\det(uF_i + G_i) = c_i(u^2 + i)$$

for $1 \le i \le 3$ and $c_1c_2c_3 = h^2$.

Fix an ordering of k. Let $1 \le i \le 3$. Since $\det(uF_i + G_i)$ is definite and $P(F_i, G_i)$ contains an isotropic form, H, with $\det(H) = -1$, it follows that $\det(uF_i + G_i)$ is negative definite. Therefore $c_i < 0$. Thus $h^2 = c_1c_2c_3 < 0$. This is a contradiction, and thus Φ is not surjective. ∎

PROPOSITION 4.9. *If Φ is surjective, then $\overline{N}_{L/k}$ is surjective for every finite extension L/k.*

Proof. In order to prove $\overline{N}_{L/k}$ is surjective, we may assume L has even degree, n, over k. We may also assume L/k is separable since L has odd degree over the separable closure of k in L.

First, assume $n \ge 6$.

Assume Φ is surjective. Let $p(x) \in k[x]$ be a monic, irreducible polynomial such that $L = k[x]/p(x)$. Let $s\colon L \to k$ be a nonzero k-linear map. Choose $e \in k^\times$.

Let $k(u, y)$ be the hyperelliptic function field defined by

$$y^2 = e \det(s_*(\langle 1\rangle))\, p(u).$$

The genus of $k(u, y)$ is at least two since $\deg(p) \ge 6$. Choose $P(F, G) \in P(k)$ such that $\Phi(P(F, G)) = k(u, y)$. Then, by Lemma 4.6, there exist $h \in k^\times$ and $F', G' \in P(F, G)$ such that

$$\det(uF' + G') = e \det(s_*(\langle 1\rangle))\, p(u) h^2.$$

By Lemma 4.3, we can find $\alpha \in L^\times$ such that

$$F' = s_*(\langle \alpha \rangle)$$
$$G' = s_*(\langle -\theta\alpha \rangle),$$

where θ is a root of $p(u)$.

By Lemmas 4.1 and 4.2,

$$\begin{aligned}\det(uF' + G') &= \det(F')p(u) \\ &= \det(s_*(\langle 1 \rangle))N_{L/k}(\alpha)p(u).\end{aligned}$$

Thus, $eh^2 = N_{L/k}(\alpha)$. This implies $\overline{N}_{L/k}(\alpha) = e(k^\times)^2$. Thus, $\overline{N}_{L/k}$ is surjective.

Now assume $n \leq 4$. If k is not real closed, then there exists a finite extension M containing L with $[M:k] \geq 6$. Thus, by the argument above, $\overline{N}_{M/k}$ is surjective and hence $\overline{N}_{L/k}$ is surjective. If k is real closed, then by Lemma 4.8, Φ is not surjective. ∎

PROPOSITION 4.10. *If Φ is surjective, then k is perfect.*

Proof. Suppose k is not perfect and let $\operatorname{char} k = p \neq 2$ with $a \in k^\times$ but $a \notin (k^\times)^p$. Let $g(u') = (u')^p - a$. Then g is irreducible over k. Let $k(u', y')$ be the hyperelliptic function field defined by $(y')^2 = g(u')$. Suppose $P(F, G) \in P(k)$ and $\Phi(P(F, G)) = k(u', y')$. Then $\det(uF + G) = f(u)$ is a square-free polynomial over k^{alg} since $\{F, G\}$ is nonsingular. Let $k(u, y)$ be the hyperelliptic function field defined by $y^2 = f(u)$. Since $k(u, y)$ and $k(u', y')$ are k-isomorphic, both function fields have the same genus, namely $(1/2)(p-1) \geq 1$. But $k^{\text{alg}}(u', y')$ has genus 0, since $g(u') = (u' - a^{1/p})^p$, and the genus of $k^{\text{alg}}(u, y)$ remains $(1/2)(p-1)$, since f is square-free over k^{alg}. This is a contradiction and therefore Φ is not surjective. ∎

Propositions 4.5, 4.9, and 4.10 now completely determine when Φ is surjective.

THEOREM 4.11. *Φ is surjective if and only if k is perfect and $\overline{N}_{L/k}$ is surjective for every finite extension L/k.*

5. INJECTIVITY

LEMMA 5.1. *Let $\{F, G\}$ and $\{F', G'\}$ be two nonsingular pairs of quadratic forms defined over k. Suppose every finite extension of k is quadratically closed. If $\det(uF + G) = e^2 \det(uF' + G')$ for some $e \in k^\times$, then the pairs $\{F, G\}$ and $\{F', G'\}$ are equivalent.*

Proof. Let $\det(uF' + G') = c\prod_{i=1}^{m} p_i(u)$ where the $p_i(u)$ are monic, irreducible polynomials in $k[u]$ and $c \in k^\times$, and let $\det(uF + G) = e^2 \det(uF' + G')$ for some $e \in k^\times$.

Let $L_i = k[x]/p_i(x)$ and let $s_i\colon L_i \to k$ be nonzero k-linear maps for $1 \le i \le m$.

Then, by Lemmas 4.7 and 4.3 there exist $\alpha_i, \beta_i \in L_i^\times$ and $\theta_i \in L_i$ with θ_i a root of $p_i(x)$ such that

$$F = \perp_{i=1}^{m} (s_i)_*(\langle \alpha_i \rangle),$$

$$G = \perp_{i=1}^{m} (s_i)_*(\langle -\theta_i \alpha_i \rangle),$$

$$F' = \perp_{i=1}^{m} (s_i)_*(\langle \beta_i \rangle),$$

and

$$G' = \perp_{i=1}^{m} (s_i)_*(\langle -\theta_i \beta_i \rangle).$$

Since each L_i is quadratically closed, there exists $\gamma_i \in L_i^\times$ such that $\alpha_i = \gamma_i^2 \beta_i$. Thus by Lemma 4.4, we have that the pair

$$\{(s_i)_*(\langle \alpha_i \rangle), (s_i)_*(\langle -\theta_i \alpha_i \rangle)\}$$

is equivalent to the pair

$$\{(s_i)_*(\langle \beta_i \rangle), (s_i)_*(\langle -\theta_i \beta_i \rangle)\}$$

for all $1 \le i \le m$. Thus, the pairs $\{F, G\}$ and $\{F', G'\}$ are equivalent. ∎

PROPOSITION 5.2. *If every finite extension of k is quadratically closed, then Φ is injective.*

Proof. Assume every finite extension of k is quadratically closed and suppose $\Phi(P(F_1, G_1)) = \Phi(P(F_2, G_2))$ with $P(F_2, G_2)$ having order n.

Suppose $\det(uF_1 + G_1)$ has degree four in $k[u]$. Then F_1 has order four. Since every finite extension of k is quadratically closed, $\det(uF_1 + G_1)$ is not irreducible, and thus has a root in k. Thus, there exist $F', G' \in P(F_1, G_1)$ such that

$$\det(uF' + G')$$

is a polynomial of degree three in $k[u]$.

Thus, we may assume without loss of generality that $\det(uF_1 + G_1)$ does not have degree four in $k[u]$. Similarly, we may assume that $\det(uF_2 + G_2)$ does not have degree four in $k[u]$.

By Lemma 4.6, there exist $h \in k^\times$ and $F_1', G_1' \in P(F_1, G_1)$ such that

$$\det(uF_1' + G_1') = h^2 \det(uF_2 + G_2).$$

By Lemma 5.1, we have that the pairs $\{F_1', G_1'\}$ and $\{F_2, G_2\}$ are equivalent. Thus, the pencils $P(F_1, G_1)$ and $P(F_2, G_2)$ are equivalent. ∎

PROPOSITION 5.3. *If* Φ *is injective, then* $k = k^2$.

Proof. Suppose $k \neq k^2$. We will proceed by cases.

First suppose that $-1 \notin (k^\times)^2$ and $a^2 + b^2 \in k^2$ for all $a, b \in k$. Then, k is a formally real pythagorean field. Let

$$F_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$
$$G_1 = x_1^2 - x_2^2 + 2x_3^2 + 4x_4^2,$$
$$F_2 = x_1^2 - x_2^2 + x_3^2 - x_4^2,$$

and

$$G_2 = x_1^2 + x_2^2 + 2x_3^2 - 4x_4^2.$$

Since the pair $\{F_1, G_1\}$ has only the trivial common zero and the pair $\{F_2, G_2\}$ has $(1, 1, 1, 1)$ as a nontrivial common zero, it follows that $P(F_1, G_1)$ is not equivalent to $P(F_2, G_2)$.

Since

$$\det(uF_1 + G_1) = \det(uF_2 + G_2) = (u + 1)(u - 1)(u + 2)(u + 4),$$

it follows that both pairs $\{F_1, G_1\}$ and $\{F_2, G_2\}$ are nonsingular and

$$\Phi\big(P(F_1, G_1)\big) = \Phi\big(P(F_2, G_2)\big).$$

Thus, in this case, Φ is not injective.

Now we must consider either $-1 \notin (k^\times)^2$ and $a^2 + b^2 \notin (k^\times)^2$ for some $a, b \in k$, or $-1 \in (k^\times)^2$. If $-1 \in (k^\times)^2$, then since $k \neq k^2$ there exists $d \notin (k^\times)^2$ with $-d \notin (k^\times)^2$.

Thus, in either of the remaining cases, there exists $d \notin (k^\times)^2$ and $a, b \in k$ such that $a^2 - db^2 \notin k^2$. Choose such d, a, and b. Let, $\theta = (1 + \sqrt{d})^2$. Let $p(x)$ be the minimal polynomial of θ, and let $L = k[x]/p(x)$. Let $s\colon L \to k$ be a nonzero k-linear map. Let

$$F_1 = s_*(\langle 1 \rangle) \perp x_3^2,$$
$$G_1 = s_*(\langle -\theta \rangle) \perp x_4^2,$$
$$F_2 = s_*\big(\langle a + b\sqrt{d}\,\rangle\big) \perp x_3^2,$$

and

$$G_2 = s_*\Big(\big\langle -\big(a + b\sqrt{d}\,\big)\theta\big\rangle\Big) \perp (a^2 - db^2)x_4^2.$$

By Lemmas 4.1 and 4.2, $\det(uF_1 + G_1) = \det(s_*(\langle 1\rangle))p(u)u$ and

$$\det(uF_2 + G_2) = \det(s_*(\langle 1\rangle))\,p(u)u(a^2 - db^2)^2.$$

Thus, $P(F_1, G_1) \in P(k)$, $P(F_2, G_2) \in P(k)$, and $\Phi(P(F_1, G_1)) = \Phi(P(F_2, G_2))$.

Let $A, B \in k^\times$. Then the order of $AF_1 + BG_1$ is four. But the orders of both F_2 and G_2 are three. Thus, if $P(F_1, G_1)$ is equivalent to $P(F_2, G_2)$, then either

1. $\{F_2, G_2\}$ is equivalent to $\{AF_1, BG_1\}$ or
2. $\{F_2, G_2\}$ is equivalent to $\{AG_1, BF_1\}$.

Considering F_1, G_1, F_2, and G_2 as forms in three variables, we have

$$\det(F_1) = \det(s_*(\langle 1\rangle)),$$

$$\det(G_1) = N_{L/k}(\theta)\det(s_*(\langle 1\rangle)),$$

$$\det(F_2) = (a^2 - db^2)\det(s_*(\langle 1\rangle)), \quad \text{and}$$

$$\det(G_2) = (a^2 - db^2)^2 N_{L/k}(\theta)\det(s_*(\langle 1\rangle)).$$

Suppose first that $\{F_2, G_2\}$ is equivalent to $\{AF_1, BG_1\}$. The equivalence of F_2 and AF_1 implies $\det(F_2) \in \det(AF_1)(k^\times)^2$, so $A \in (a^2 - db^2)(k^\times)^2$. The equivalence of G_2 and BG_1 implies $\det(G_2) \in \det(BG_1)(k^\times)^2$, so $B \in (k^\times)^2$. Thus,

$$AB \in (a^2 - db^2)(k^\times)^2.$$

The equivalence of $\{F_2, G_2\}$ and $\{AF_1, BG_1\}$ implies

$$\det(uF_2 + G_2) \in \det(uAF_1 + BG_1)(k^\times)^2.$$

The coefficient of u^3 in $\det(uAF_1 + BG_1)$ is $A^2 \det(s_*(\langle 1\rangle))AB$. The coefficient of u^3 in $\det(uF_2 + G_2)$ is $(a^2 - db^2)^2 \det(s_*(\langle 1\rangle))$. Therefore, $AB \in (k^\times)^2$.

Therefore, $a^2 - db^2 \in (k^\times)^2$. This contradicts our choices of a, b, and d. Thus, $\{F_2, G_2\}$ is not equivalent to $\{AF_1, BG_1\}$.

Now, suppose that $\{F_2, G_2\}$ is equivalent to $\{AG_1, BF_1\}$. The equivalence of F_2 and AG_1 implies $AN_{L/k}(\theta) \in (a^2 - db^2)(k^\times)^2$. The equivalence of G_2 and BF_1 implies $B \in N_{L/k}(\theta)(k^\times)^2$. Thus, $AB \in (a^2 - db^2)(k^\times)^2$.

The equivalence of $\{F_2, G_2\}$ and $\{AG_1, BF_1\}$ implies

$$\det(uF_2 + G_2) \in \det(uAG_1 + BF_1)(k^\times)^2.$$

The coefficient of u^3 in $\det(uAG_1 + BF_1)$ is $A^2 N_{L/k}(\theta)\det(s_*(\langle 1\rangle))AB$. The coefficient of u^3 in $\det(uF_2 + G_2)$ is $(a^2 - db^2)^2 \det(s_*(\langle 1\rangle))$. Therefore,

$$ABN_{L/k}(\theta) \in (k^\times)^2.$$

Therefore, $N_{L/k}(\theta) \in (a^2 - db^2)(k^\times)^2$. By our choice of θ, $N_{L/k}(\theta) \in (k^\times)^2$. Thus, $a^2 - db^2 \in (k^\times)^2$. This contradicts our choices of a, b, and d. Thus, $\{F_2, G_2\}$ is not equivalent to $\{AG_1, BF_1\}$.

Therefore, if $k \neq k^2$, then Φ is not injective. ∎

LEMMA 5.4. *The following are equivalent.*

1. *Every finite extension of k is quadratically closed.*
2. *Every finite separable extension of odd degree over k is quadratically closed.*

Proof. (1) implies (2) is clear.

Assume every finite separable extension of odd degree over k is quadratically closed. Let L/k be a finite extension. Let L_s be the maximal separable extension of k in L. Let M be a Galois closure of L_s/k. Let E be a subfield of M containing k that corresponds to a Sylow 2-subgroup of $\mathrm{Gal}(M/k)$. Then $[E:k]$ is odd and M is obtained from E by a tower of quadratic extensions, since the 2-group $\mathrm{Gal}(M/E)$ has a chain of subgroups

$$1 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}(M/E),$$

with $[H_i : H_{i-1}] = 2$, $1 \leq i \leq n$.

Since E is quadratically closed, it follows that $E = M$. Thus $[M:k] = [E:k]$ is odd. It follows that $[L_s:k]$ is odd. Thus, L_s is quadratically closed by assumption.

Let $\alpha \in L^\times$. Then, $\alpha^{p^n} \in L_s^\times = (L_s^\times)^2$ for some $n \geq 0$, where $\mathrm{char}\, k = p$. Thus, $\alpha(\alpha^{(p^n-1)/2})^2 = \alpha^{p^n} = b^2$ for some $b \in L_s^\times$. Thus $\alpha \in (L^\times)^2$. Therefore, L is quadratically closed. ∎

PROPOSITION 5.5. *If Φ is injective, then every finite extension of k is quadratically closed.*

Proof. Assume Φ is injective. Let L/k be a finite separable extension of odd degree, $[L:k] = n$. Let $p(x)$ be a monic, irreducible polynomial such that

$$L = k[x]/p(x).$$

Let $s\colon L \to k$ be the trace map $\mathrm{Tr}_{L/k}$. Since L/k is separable, s is nonzero.

Choose $c \in L^\times$ and $\theta \in L$ a root of $p(x)$.

Let

$$F_1 = s_*(\langle 1\rangle) \perp 0x_{n+1}^2,$$

$$G_1 = s_*(\langle -\theta\rangle) \perp x_{n+1}^2,$$

$$F_2 = s_*(\langle c\rangle) \perp 0x_{n+1}^2,$$

and

$$G_2 = s_*(\langle -c\theta\rangle) \perp x_{n+1}^2.$$

By Lemmas 4.1 and 4.2, $\det(uF_1 + G_1) = \det(s_*(\langle 1\rangle))N_{L/k}(1)p(u)$ and $\det(uF_2 + G_2) = \det(s_*(\langle 1\rangle))N_{L/k}(c)p(u)$. Thus, both pairs $\{F_1, G_1\}$ and $\{F_2, G_2\}$ are nonsingular, both pairs have even order, and since $N_{L/k}(c) \in (k^\times)^2$, by Proposition 5.3, it follows that

$$\Phi\big(P(F_1, G_1)\big) = \Phi\big(P(F_2, G_2)\big).$$

Since Φ is injective, $P(F_1, G_1)$ is equivalent to $P(F_2, G_2)$. Since the order of $AF_1 + BG_1$ is

$$\begin{array}{ll} n+1 & \text{if } B \neq 0 \\ n & \text{if } A \neq 0,\ B = 0, \end{array}$$

it follows that the pairs $\{AF_1, BF_1 + CG_1\}$ and $\{F_2, G_2\}$ are equivalent for some $A, B, C \in k$ with $A, C \neq 0$.

We see that

$$AF_1 = s_*(\langle A\rangle) \perp 0x_{n+1}^2$$

and

$$BF_1 + CG_1 = s_*\left(\left\langle -A\left(\frac{C\theta - B}{A}\right)\right\rangle\right) \perp Cx_{n+1}^2.$$

Since

$$\det(uAF_1 + BF_1 + CG_1) = \alpha^2 \det(uF_2 + G_2)$$

for some $\alpha \in k^\times$, it follows that $(C\theta - B)/A$ is a root of $p(u)$. Thus, there exists a k-automorphism

$$\tau\colon L \to L$$

with $\tau(\theta) = (C\theta - B)/A$.

For any $\beta \in L$, $s(\beta) = s(\tau(\beta))$ since β and $\tau(\beta)$ have the same trace. For any $u, v \in L$,

$$\begin{aligned}\rho_A(u)(v) &= s(Auv) = s(\tau(Auv)) = s(A\tau(u)\tau(v)) \\ &= \rho_A(\tau(u))(\tau(v)),\end{aligned}$$

and

$$\begin{aligned}\rho_{-A\theta}(u)(v) &= s(-A\theta uv) \qquad\qquad = s(\tau(-A\theta uv)) \\ &= s\left(-A\frac{C\theta - B}{A}\tau(u)\tau(v)\right) = \rho_{-[A(C\theta-B)/A]}(\tau(u))(\tau(v)).\end{aligned}$$

Thus, by Lemma 4.4 and since $C \in k = k^2$, the pairs $\{AF_1, BF_1 + CG_1\}$ and

$$\left\{s_*(\langle A\rangle) \perp 0x_{n+1}^2, s_*(\langle -A\theta\rangle) \perp x_{n+1}^2\right\}$$

are equivalent. Therefore, the pairs $\{F_2, G_2\}$ and

$$\left\{s_*(\langle A\rangle) \perp 0x_{n+1}^2, s_*(\langle -A\theta\rangle) \perp x_{n+1}^2\right\}$$

are equivalent. Thus, by Lemma 4.4, $c = \gamma^2 A$ for some $\gamma \in L^\times$. Since

$$A \in k^\times = (k^\times)^2 \subseteq (L^\times)^2,$$

it follows that $c \in (L^\times)^2$. Thus $L^\times = (L^\times)^2$ and L is quadratically closed. Lemma 5.4 implies that every finite extension of k is quadratically closed. ∎

We have completely determined when Φ is injective.

THEOREM 5.6. *Φ is injective if and only if k and every finite extension of k is quadratically closed.*

If k is quadratically closed, then it is clear that every norm map $\overline{N}_{L/k}$ is surjective. Therefore, Propositions 4.5 and 5.3 imply that if k is perfect and Φ is injective, then Φ is surjective. This gives our main result.

THEOREM 5.7. *Let k be a perfect field with* $\operatorname{char} k \neq 2$. *The following statements are equivalent.*

1. *Φ is injective.*
2. *Φ is bijective.*
3. *k and every finite extension of k is quadratically closed.*

REFERENCES

1. C. Chevalley, "Introduction to the Theory of Algebraic Functions of One Variable," Amer. Math. Soc., Providence, 1951.
2. R. Hartshorne, "Algebraic Geometry," GTM #52, Springer-Verlag, New York, 1977.
3. F. Ischebeck and W. Scharlau, Hermitesche und orthogonale Operatoren über kommutativen Ringen, *Math. Ann.* **200** (1973), 327–334.
4. T. Lam, "The Algebraic Theory of Quadratic Forms," Mathematics Lecture Note Series, Benjamin, Reading, MA, 1973.
5. D. Leep and L. Schueller, Classification of pairs of symmetric and alternating bilinear forms, *Exposition Math.* **17** (1999), 385–414.
6. W. Scharlau, "Quadratic and Hermitian Forms," Grundlehren der mathematischen Wissenschaften, Vol. 270, Springer-Verlag, Berlin, 1985.
7. L. Schueller, "Pairs of Quadratic Forms Over Arbitrary Fields," Ph.D. dissertation, University of Kentucky, 1996.
8. H. Stichtenoth, "Algebraic Function Fields and Codes," Universitext, Springer-Verlag, Berlin/Heidelberg, 1993.
9. W. Waterhouse, Pairs of quadratic forms, *Invent. Math.* **37** (1976), 157–164.
10. A. Weil, Footnote to a Recent Paper, *Amer. J. Math.* **76** (1954), 347–350.